Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 October 2026

Vulnerabilities

PHP2Shell: Suspected North Korean campaign targets 216 vulnerable PHP hosts

Security Affairs - 26 October 2026 10:58

Cyfirma links PHP2Shell scans of 216 vulnerable hosts to a suspected North Korean campaign using AI to rank public exploits. On October 21, PHP released emergency patches for two critical vulnerabilities, CVE-2026-109618 and CVE-2026-109619, both rated 9.2 on the CVSS scale.

Critical 'HTTP2Shell' Brotli vulnerability triggers emergency patches

BleepingComputer - 26 October 2026 13:27

A critical flaw dubbed 'HTTP2Shell' in Brotli, the C decoder library built into Node.js, could allow attackers to corrupt memory and access sensitive data.

Two Critical Wasmtime Flaws Could Let Malicious WebAssembly Modules Escape Sandboxes

The Hacker News - 26 October 2026 18:22

Two critical flaws in Wasmtime, a WebAssembly runtime that can be built into other software, could allow a malicious WebAssembly module to escape the sandbox intended to contain it, the project's maintainers say.

Linux Flaws Exposed Before Fixes as Root Exploit Goes Public

Infosecurity Magazine - 26 October 2026 15:00

Six Linux flaws were made public, including one with a working root exploit and no merged fix.

Threat actors and malware

Microsoft 365 Token-Replay Attacks Compromise 97 Accounts at 79 Organizations

The Hacker News - 26 October 2026 15:05

Cybersecurity researchers have disclosed a Microsoft 365 campaign that has been observed leveraging an adversary-in-the-middle (AitM) relay to capture sign-in sessions and then replay the stolen tokens to break into email accounts at 79 organizations.

Scottish Cyber Coordination Centre

Hackers Infect 953 Online Stores With Scanner-Evading JavaScript, Mostly on Magento

The Hacker News - 27 October 2026 00:42

An unknown threat actor has infected 953 online stores, most of them running Magento, as part of a long-running campaign active since July 2025. According to Dutch e-commerce security company Sansec, the activity is designed to add a small piece of code to the store's pages that, when visited by unsuspecting users, serves malicious JavaScript loader code through Magento CMS blocks.

Researchers Uncover Rentable Android Spyware uCreater Targeting WeChat and Telegram

Security Affairs - 26 October 2026 13:11

uCreater is Android spyware disguised as trusted apps, stealing credentials, messages and wallet data through a rentable platform. uCreater is a rentable Android spyware platform that hides inside repackaged legitimate apps, targeting messaging services and mobile wallets.

Attackers Use Microsoft Teams IT Support Scams to Deploy Malware and Ransomware

The Hacker News - 26 October 2026 22:22

Cybersecurity researchers are calling attention to what they say is a "recurring social engineering pattern" across hundreds of cases in which threat actors use Microsoft Teams' external chat creation feature to conduct impersonation scams or to deliver malware.

In-the-Wild Attack Abuses AI Agents' Trust in Markdown

darkreading - 26 October 2026 21:59

A new AI agent prompt injection technique exploits how coding assistants consume local instruction files, blurring the line between text documents and executable actions.